[redacted]

04-36
01-92

---------- Original Message ----------
Subject: VOIP technology allows easy ani caller-id spoofing
From: paulickj@duq.edu
Date: Mon, November 28, 2005 10:53 am
To: fccinfo@fcc.gov
Cc: KJMWEB@fcc.gov

Dear FCC,

Firstly, I am copying the chairman because I believe this concern is of great importance for all people who use telephones, which would be a great majority of Americans.

I've recently been experiencing prank phone calls from fake phone numbers and phone numbers of people that would not prank call me, i.e. I've identified the calling number, contacted the callers and verified that they were not the original callers. So I've done some research to figure out, how could it be that when I dialed *69 to retrieve the number of the last incoming call, I got a number that couldn't possibly have been the prank caller.

I've discovered the following:

Until VOIP came into the picture, it's been extremely difficult to spoof the ani-caller id number from a telephone, i.e. it involved expensive equipment and considerable technical skill.

Now that voip is completely wired to our public telephone network, all of the hacking and cracking that was present in the internet has now "wormed" its way into our public telephone network. It is very analogous to connecting an insecure private network directly to the internet without a firewall. Before the private network was attached to the internet, very few security related breaches would occur. Then, when the private network is connected to the internet, all of the hacking that could not reach the private network now has free access to the unprepared private network.

How is this a relevant analogy?

Our public telephone network was actually kind of private, i.e. it was not connected to the internet in such a manner that allowed direct interface by internet users.

Now, because the public telephone network is unprepared to deal with the new interfacing that voip has with the public telephone network, it is also unprepared to deal with all of the maladies on the internet, e.g. spoofing, phishing, hacking and cracking.

Though the FCC does not regulate Voice over IP, voice over IP is now inextricably connected to our public telephone network, and any actions that are used to subvert or "hack" the voip network is going to necessarily collaterally attack the public telephone network (which is regulated by the FCC).

I am writing this concern because A. I've now experienced the helpless state of not being able to trace the call back to the prank caller and B. I recognize that this is probably going to become more widespread as voip expands.

Below are some links that explain how simple this caller ID spoofing is with a simple voip connection and a personal computer. These tools (internet conection + computer) are pretty standard among all american households. Given the undying popularity of prankcalling, the prankster's now have an even more powerful tool to use to cover their

tracks and cause more confusion with no recourse by the victim.

Please give this technological backdoor considerable concern before it becomes a major problem. Sooner or later, this information will become mainstream and every kid that doesn't have enough time on his/her hands will be doing this for fun.

Again, I experienced this first hand….this is not a concern in a vacuum full of hypotheticals.

I searched the fcc.gov website for anything related to voip ani caller-id spoofing and I found nothing.

Here are some articles that explain how this backdoor is exploited.

Regards,
-Jim Paulick

http://www.theregister.co.uk/2004/07/07/hackers_gut_voip/

http://blog.tmcnet.com/blog/tom-keating/voip/callerid-spoofing.asp

http://www.wired.com/news/privacy/0,1848,66954,00.html